CLAIMS

What is claimed is:

1. A method for preventing denial of service attacks against Hypertext Transfer Protocol (HTTP) servers, comprising:

receiving a HTTP request from a subscriber using a first communication network coupled to at least one other communication network, said request including a Universal Resource Locator (URL);

receiving a profile for said subscriber;

filtering said request to determine whether said subscriber is authorized to make said request based upon said profile; and

forwarding said request to said at least one other communication network when said subscriber is authorized to make said request.

2. The method of claim 1 wherein said filtering further comprises:

updating a client HTTP request count when said request is a HTTP "GET" request or a HTTP "POST" request; and

applying HTTP server attack preventative measures when said request count exceeds a maximum HTTP request count.

3. The method of claim 2 wherein said applying further comprises setting an alarm when said request count exceeds said maximum HTTP request count.

4. The method of claim 3, further comprising sending said alarm to an Internet Service Provider (ISP) associated with said subscriber.

5. The method of claim 2 wherein said applying further comprises dropping the data packet containing said request when said request count exceeds said maximum HTTP request count.

6. The method of claim 2 wherein said applying further comprises shutting down the account used to access said first communication network when said request count exceeds said maximum HTTP request count.

7. The method of claim 6 wherein said applying further comprises disabling HTTP requests for a hold-down period when said request count exceeds said maximum HTTP request count.

8. The method of claim 7, further comprising increasing said hold-down period each time said HTTP count exceeds said maximum HTTP request count.

9. The method of claim 8 wherein said hold-down period increases exponentially each time said HTTP count exceeds said maximum HTTP request count.

10. The method of claim 1 wherein said filtering further comprises indicating said request is unauthorized when the HTTP request frequency exceeds a maximum HTTP request frequency.

11. The method of claim 1 wherein said filtering further comprises indicating said request is unauthorized when the frequency of HTTP requests for said URL exceeds a maximum HTTP request frequency.

12. A program storage device readable by a machine, embodying a program of instructions executable by the machine to perform a method to prevent denial of service attacks against Hypertext Transfer Protocol (HTTP) servers, the method comprising:

receiving a HTTP request from a subscriber using a first communication network coupled to at least one other communication network, said request including a Universal Resource Locator (URL);

receiving a profile for said subscriber;

filtering said request to determine whether said subscriber is authorized to make said request based upon said profile; and

forwarding said request to said at least one other communication network when said subscriber is authorized to make said request.

13. The program storage device of claim 12 wherein said filtering further comprises:

updating a client HTTP request count when said request is a HTTP "GET" request or a HTTP "POST" request; and

applying HTTP server attack preventative measures when said request count exceeds a maximum HTTP request count.

14. The program storage device of claim 13 wherein said applying further comprises setting an alarm when said request count exceeds said maximum HTTP request count.

15. The program storage device of claim 14, further comprising sending said alarm to an Internet Service Provider (ISP) associated with said subscriber.

16. The program storage device of claim 13 wherein said applying further comprises dropping the data packet containing said request when said request count exceeds said maximum HTTP request count.

17. The program storage device of claim 13 wherein said applying further comprises shutting down the account used to access said first communication network when said request count exceeds said maximum HTTP request count.

18. The program storage device of claim 17 wherein said applying further comprises disabling HTTP requests for a hold-down period when said request count exceeds said maximum HTTP request count.

19. The program storage device of claim 18, further comprising increasing said hold-down period each time said HTTP count exceeds said maximum HTTP request count.

20. The program storage device of claim 19 wherein said hold-down period increases exponentially each time said HTTP count exceeds said maximum HTTP request count.

21. The program storage device of claim 12 wherein said filtering further comprises indicating said request is unauthorized when the HTTP request frequency exceeds a maximum HTTP request frequency.

22. The program storage device of claim 12 wherein said filtering further comprises indicating said request is unauthorized when the frequency of HTTP requests for said URL exceeds a maximum HTTP request frequency.

23. An apparatus for preventing denial of service attacks against Hypertext Transfer Protocol (HTTP) servers, the apparatus comprising:

means for receiving a HTTP request from a subscriber using a first communication network coupled to at least one other communication network, said request including a Universal Resource Locator (URL);

means for receiving a profile for said subscriber;

means for filtering to determine whether said subscriber is authorized to make said request based upon said profile; and

means for forwarding said request to said at least one other communication network when said subscriber is authorized to make said request.

24. The apparatus of claim 23 wherein said means for filtering further comprises:

means for updating a client HTTP request count when said request is a HTTP "GET" request or a HTTP "POST" request; and

means for applying HTTP server attack preventative measures when said request count exceeds a maximum HTTP request count.

25. The apparatus of claim 24 wherein said means for applying further comprises means for setting an alarm when said request count exceeds said maximum HTTP request count.

26. The apparatus of claim 25, further comprising means for sending said alarm to an Internet Service Provider (ISP) associated with said subscriber.

27. The apparatus of claim 24 wherein said means for applying further comprises means for dropping the data packet containing said request when said request count exceeds said maximum HTTP request count.

28. The apparatus of claim 24 wherein said means for applying further comprises means for shutting down the account used to access said first communication network when said request count exceeds said maximum HTTP request count.

29. The apparatus of claim 28 wherein said means for applying further comprises means for disabling HTTP requests for a hold-down period when said request count exceeds said maximum HTTP request count.

30. The apparatus of claim 29, further comprising means for increasing said hold-down period each time said HTTP count exceeds said maximum HTTP request count.

31. The apparatus of claim 30 wherein said hold-down period increases exponentially each time said HTTP count exceeds said maximum HTTP request count.

32. The apparatus of claim 23 wherein said means for filtering further comprises means for indicating said request is unauthorized when the HTTP request frequency exceeds a maximum HTTP request frequency.

33. The apparatus of claim 23 wherein said filtering further comprises means for indicating said request is unauthorized when the frequency of HTTP requests for said URL exceeds a maximum HTTP request frequency.

34. An apparatus capable of preventing denial of service attacks against Hypertext Transfer Protocol (HTTP) servers, said apparatus comprising:

a profile request generator capable of generating a profile request based upon a HTTP request received from a subscriber using a first communication network, said request including a Universal Resource Locator (URL);

a filter capable of determining whether said request is authorized based upon said requested profile; and

an authorizer capable of allowing said request said request to be forwarded on at least one other communication network coupled to said first communication network.

35. The apparatus of claim 34, further comprising:

a first receiving interface capable of accepting said request;

a first forwarding interface capable of sending said profile request to an AAA server;

a second receiving interface capable of accepting a requested profile; and

a second forwarding interface capable of forwarding said request on said at least one other communication network.

36. The apparatus of claim 35 wherein said filter further comprises:

an updater to update a client HTTP request count when said request is a HTTP "GET" request or a HTTP "POST" request; and

a responder to apply HTTP server attack preventative measures when said request count exceeds a maximum HTTP request count.

37. The apparatus of claim 36 wherein said responder further sets an alarm when said request count exceeds a maximum HTTP request count.

38. The apparatus of claim 36 wherein said responder sends said alarm to an Internet Service Provider (ISP) associated with said subscriber.

39. The apparatus of claim 36 wherein said responder drops the data packet containing said request when said request count exceeds a maximum HTTP request count.

40. The apparatus of claim 36 wherein said responder shuts down the account used to access said first communication network when said request count exceeds a maximum HTTP request count.

41. The apparatus of claim 40 wherein said responder disables HTTP requests for a hold-down period when said request count exceeds a maximum HTTP request count.

42. The apparatus of claim 41 wherein said responder increases said hold-down period each time said HTTP count exceeds said maximum HTTP request count.

43. The apparatus of claim 42 wherein said responder increases said hold-down period exponentially each time said HTTP count exceeds said maximum HTTP request count.

44. The apparatus of claim 34 wherein said filter further indicates said request is unauthorized when the HTTP request frequency exceeds a maximum HTTP request frequency.

45. The apparatus of claim 34 wherein said filter indicates said request is unauthorized when the frequency of HTTP requests for said URL exceeds a maximum HTTP request frequency.